Computer Networks & Software, Inc.

SigSec™ Discussion

Providing Innovative Technical Solutions and Professional Services To Selected Government Agencies Supporting Our Nation's Air Transport, Global Defense and Homeland Security

Computer Networks & Software, Inc.
7405 Alban Station Court
Suite B-215
Springfield, VA 22150

2007

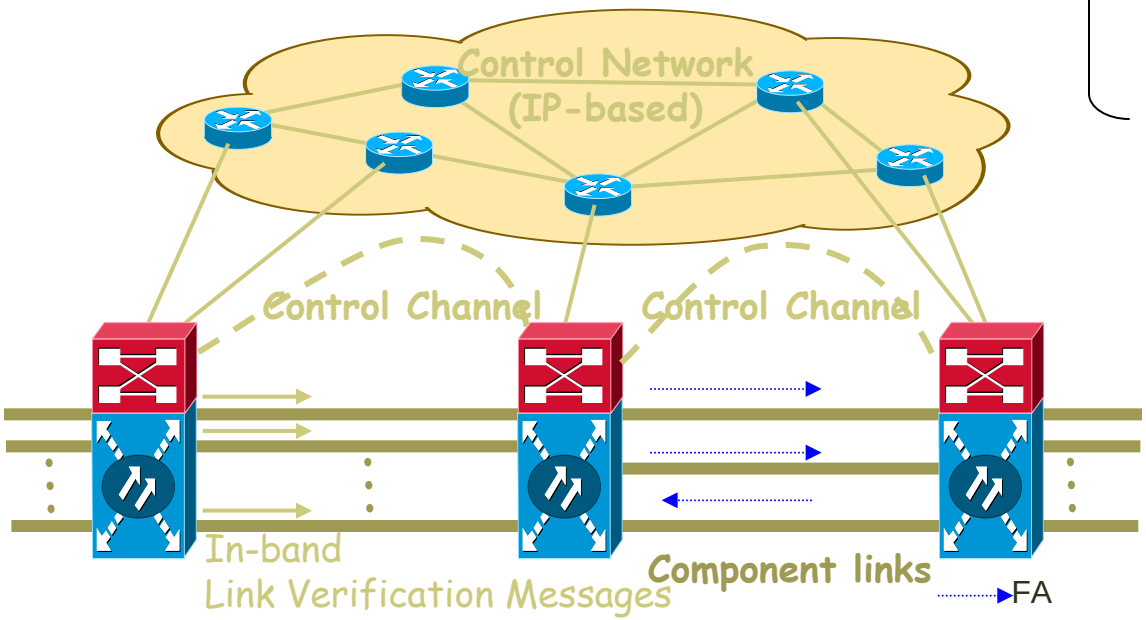
SigSec^{tm} Technology

SigSec^{tm} DOE Phase II SBIR

- An intrusion detection and prevention technology for the GMPLS Control Plane
- Prevents attacks in real time
  - Prevents zero day attacks
- Based on deep protocol analysis:
  - Syntax
  - Semantics
  - State machine techniques

GMPLS Architecture

Control Plane can be attacked by users or "inside" network management personnel



GMPLS Protocols

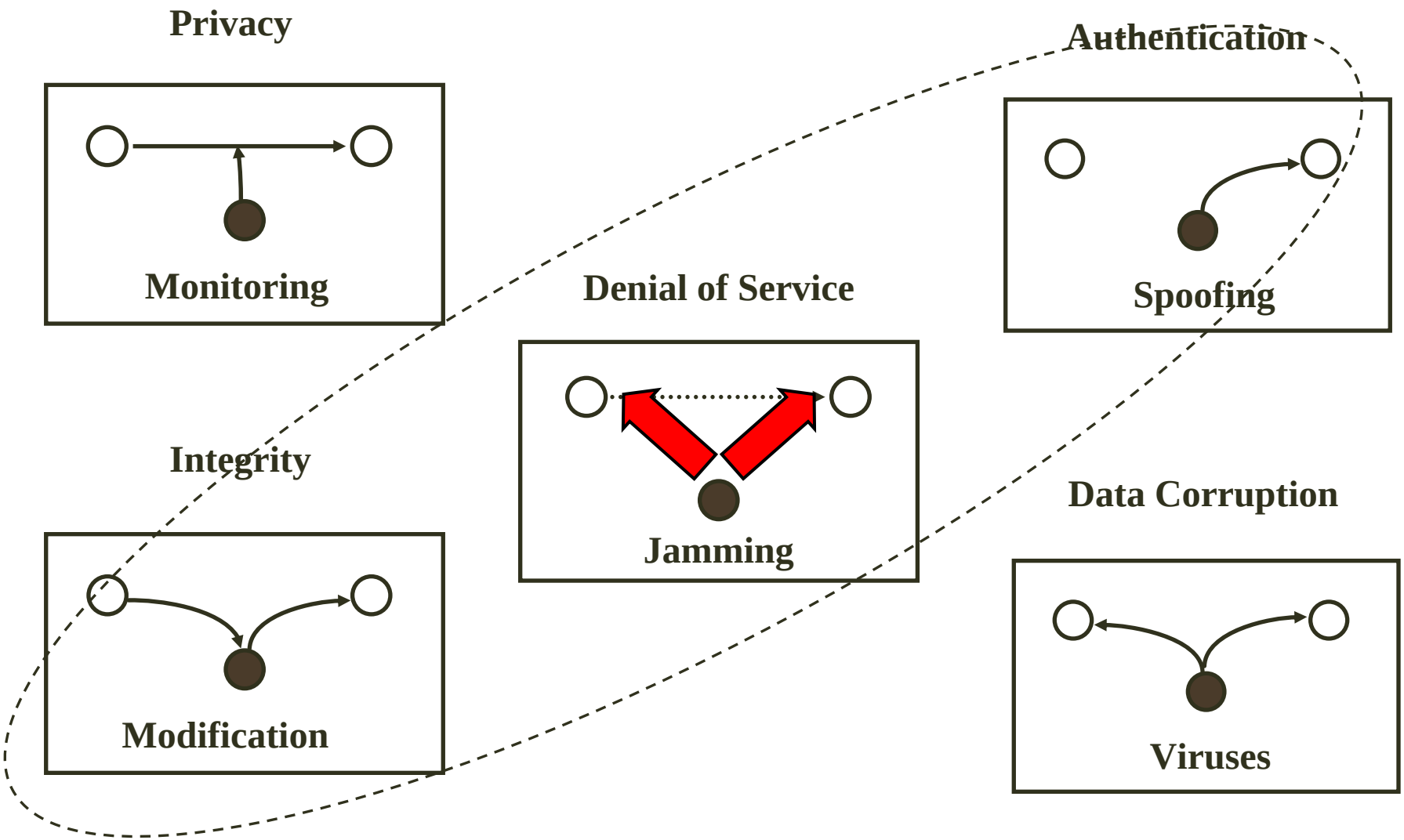
- **Link Management Protocol (LMP)**
  - **To manage the control plane link Signaling protocols**
- **Label Distribution Protocol (LDP)**
- **RSVP-Traffic Engineering (TE)**
- **Routing protocols**
  - **System (IS-IS)**
  - **Open Shortest Path First (OSPF)**
  - **Border Gateway Protocol (BGP)**

GMPLS = General Multi-label Protocol Switching

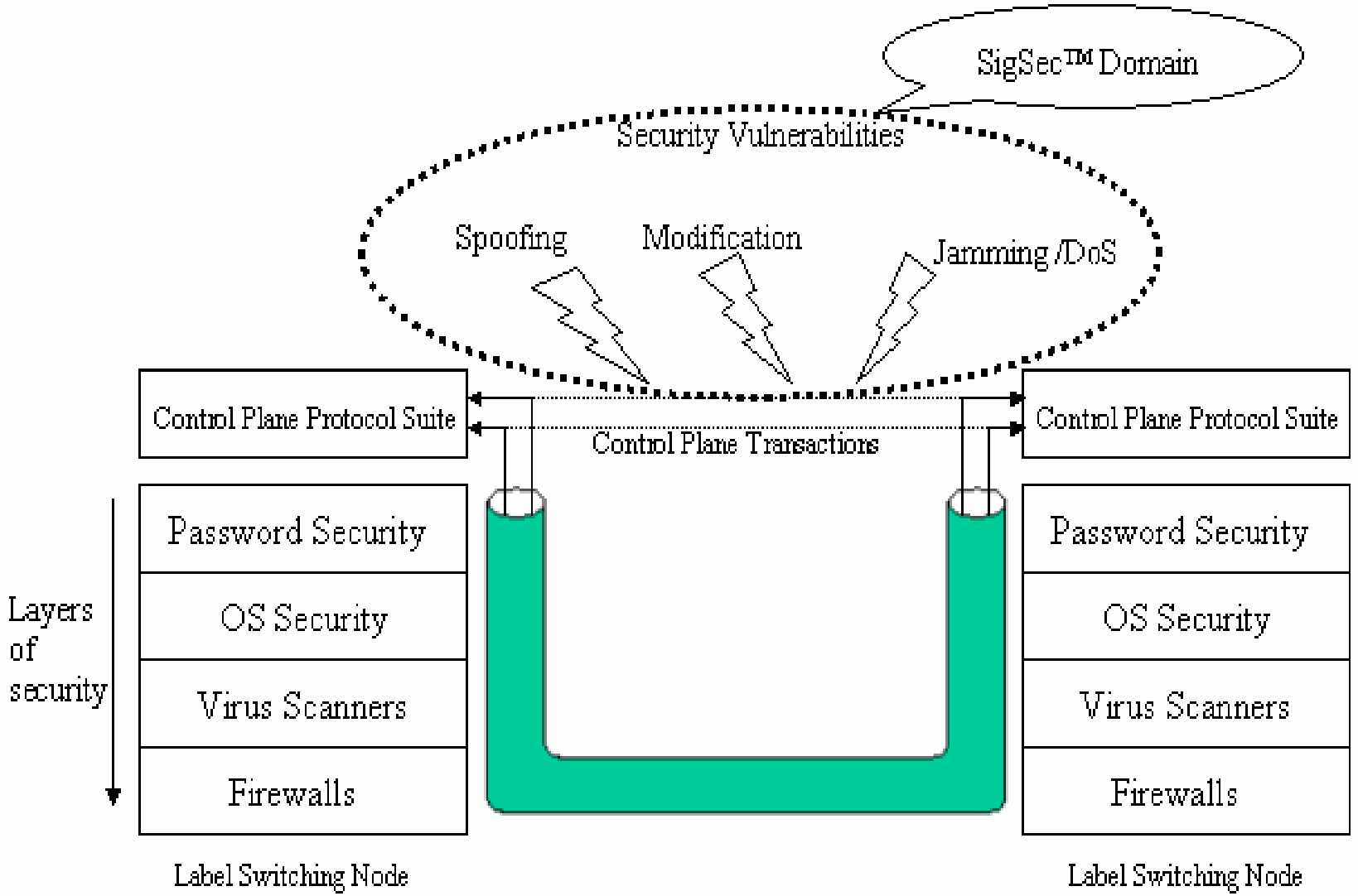
GMPLS

- Generalized Multiple Protocol Label Switching (GMPLS) extends Multi Protocol Label Switching (MPLS) to provide the control plane for devices that can switch packet, time, wavelength, and fiber domains.
- This common control plane promises to simplify network operation and management by automating end-to-end provisioning of connections, managing network resources, and providing the level of QoS that is expected in the new, sophisticated application
- The control plane utilizes a suite of protocols, including LMP, RSVP-TE, OSPF-TE, BGP, CR-LDP, IS-IS.

Intruders Basic Attacks – SigSec Domain



SigSec Domain

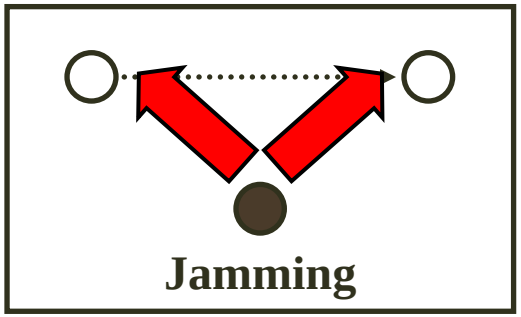


SigSec Attack Profile

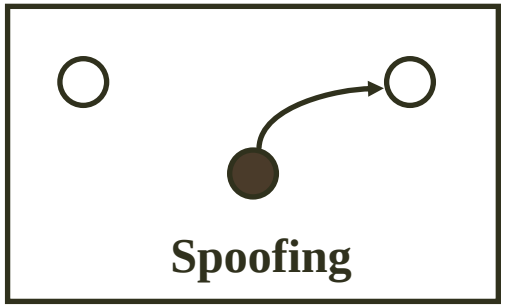
Types of Attacks (Categories)

- Denial of Service
- Protocol Exploitation (leads to other types)
- Impersonation
  - Direct Route attacks
  - Playback
- Man in the middle

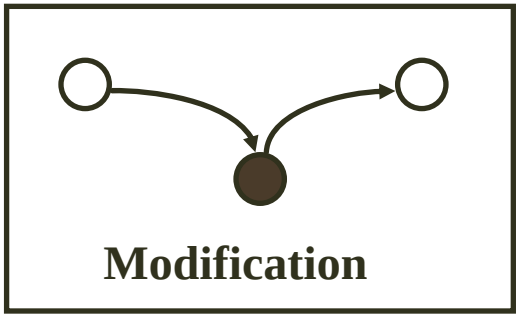
Denial of Service



Authentication



Integrity



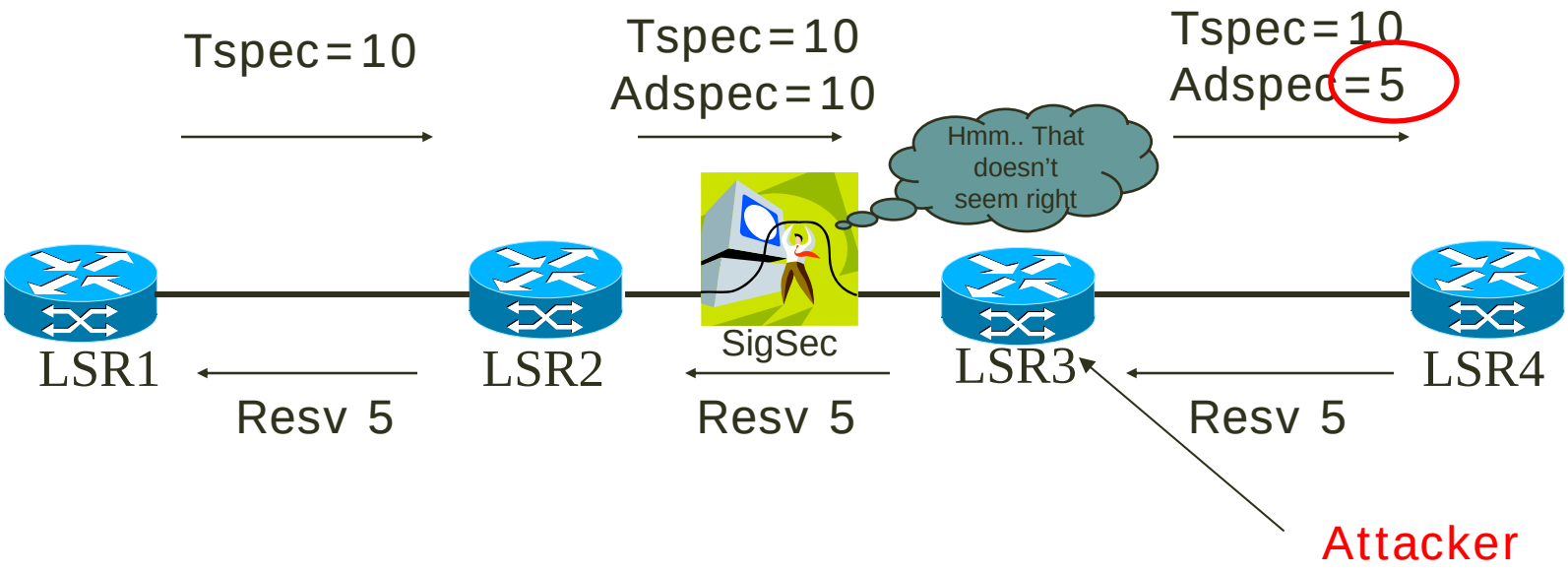
Research performed

- **Single protocol analysis**
  - **Syntax / Semantic Analysis**
  - **Finite State Machine Behavior Analysis**
- **Inter protocol Interaction**
  - **Detection of attacks on one protocol through metrics of another**
- **The number of interactions that require to be monitored is significantly lower than the number of transactions taking place in the data plane**

SigSec Capabilities

- ‘SigSec Core’ detects all known semantics and syntax related inconsistencies of the GMPLS control plane protocols
- ‘SigSec Core’ detects many known attacks that may pass through semantic and syntax analyzers
  - Using FSM analyzer that depends on attack profiles
  - Unknown attacks detected through unexpected protocol exchanges/state changes

An Attack Illustration & Detection example :RSVP



SigSec Attack Detection Capabilities – Summary

Type Of Attack	Total Number Detectable* (Numbers may change as study progresses)
Denial Of Service	60
Protocol Exploitation	10
Man In the Middle	6
Impersonation	7

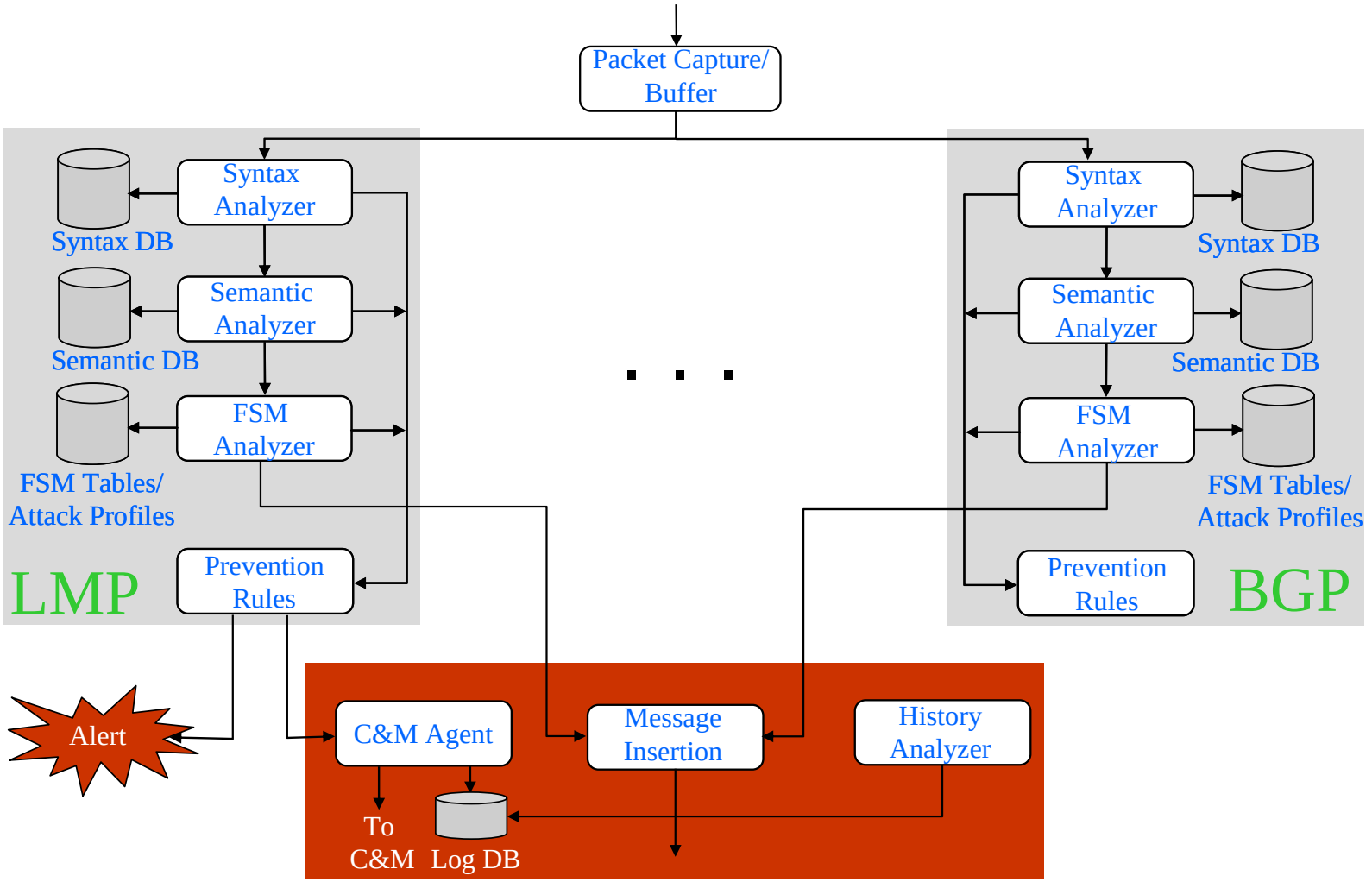
Attack Levels	# detected
Critical	**7**
High	**59**
Medium	**32**
Low	**5**

- All semantics and syntax inconsistencies will be detected (restricted by accuracy of syntax and semantics database)

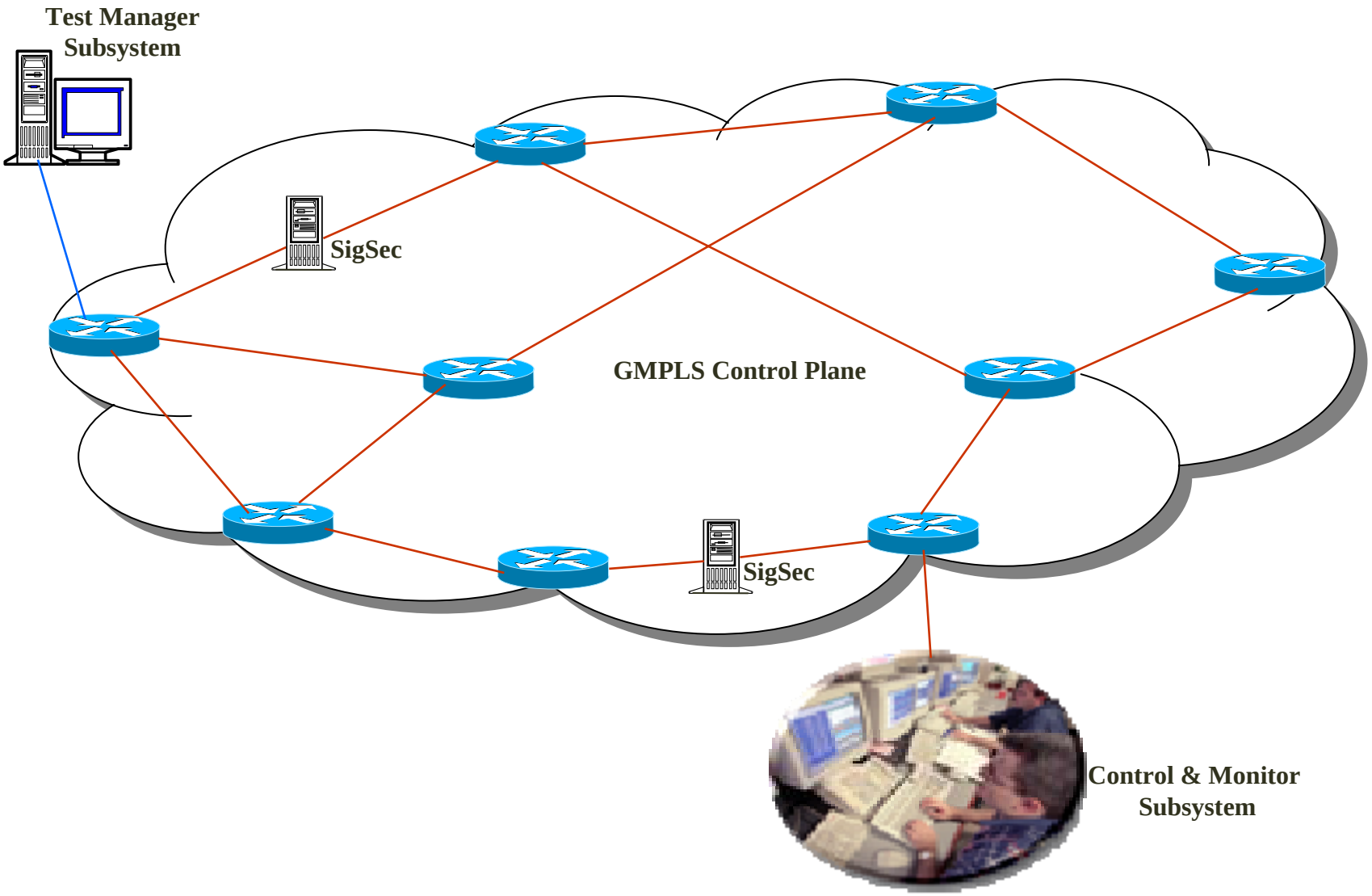
SigSec Attack Detection Capabilities – Threat Levels

Attack Threat Level	Definition
Critical	Attack that can bring about considerable down time on the network infrastructure (Area or Domain). This can bring down the data plane infrastructure and its maintenance. Attacker has the freedom to interfere with node of his choice
High	Attack brings down a certain node/router that can bring about network wide impact due to unsynchronized, wrong, bogus information.Network Level Impact may be in the form of a considerable link down time
Medium	Attack brings about a mis-allocation of system resources in a domain or area or link. Caused by congestion of a link or part of a network
Low	Attack that is usually picked up by the protocol and has effective resolution with minimal downtime of area or domain. Such attacks are also aimed at consumtion of resources

SigSec_IDS Subsystem Functional Overview



CNS Testbed Logical Architecture



Computer Networks & Software, Inc.

Thank You !

CNS, Inc